AF/IFW

TRANSMITTAL OF APPEAL BRIEF (Large Entity)

Docket No.
879A.0054.U1(US)

In Re Application Of: **Niall O'Donoghue**

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
10/608,235	06/27/2003	Lashley, Laurel L.	29683	2132	8545

Invention: **Method and Device For Authenticating A User in a Variety of Contexts**

COMMISSIONER FOR PATENTS:

Transmitted herewith is the Appeal Brief in this application, with respect to the Notice of Appeal filed on:
March 10, 2008

The fee for filing this Appeal Brief is: **$510.00**

☒ A check in the amount of the fee is enclosed.

□ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 50-1924. I have enclosed a duplicate copy of this sheet.

□ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Signature

Dated: 6/6/2008

John A. Garrity
(Reg. No. 60,470)
Harrington & Smith, PC
4 Research Drive
Shelton, CT 06484-6212

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on

June 6, 2008
(Date)

Debra Pongetti
Signature of Person Mailing Correspondence

Debra Pongetti
Typed or Printed Name of Person Mailing Correspondence

IN THE U.S. PATENT AND TRADEMARK OFFICE

Appl. No. : 10/608,235
Applicant : Niall O'Donoghue
Filed : June 27, 2003
TC/AU : 2132
Examiner : Lashley, Laurel L.

Docket No. : 879A.0054.U1(US)
Customer No. : 29683

Title : METHOD AND DEVICE FOR AUTHENTICATING A USER IN A VARIETY OF CONTEXTS

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANT'S APPEAL BRIEF

Sir:

The Applicant/Appellant hereby submits this APPEAL BRIEF to the Board of Patent Appeals and Interferences. Enclosed is a draft in the amount of $120 for a one month time extension. Should the undersigned attorney be mistaken as to time or fees, please consider this a petition for an additional extension of time under 37 C.F.R. § 1.136(a) or (b) that may be required to avoid dismissal of this appeal, and debit Deposit Account No. 50-1924 as appropriate.

TABLE OF CONTENTS

Page

(1) REAL PARTY IN INTEREST

The real party in interest (RPI) is Nokia Corporation of Espoo, Finland, as evidenced by an assignment filed on June 27, 2003 and recorded on October 22, 2003 at reel /frame 014612/0486.

(2) RELATED APPEALS AND INTERFERENCES

There are no other pending appeals or interferences of which the undersigned representative and assignee/RPI is aware that will directly affect, be directly affected by or have a bearing on the Board's decision in this appeal.

(3) STATUS OF CLAIMS

Claims 1-14 are pending in this appeal, and are reproduced in an Appendix beginning at page 22 of this Brief as those claims stood finally rejected by an Office Action dated January 8th, 2008. All claims are rejected.

This application was filed with claims 1-14. In response to a first non-final Office Action dated July 24, 2006 that rejected each of claims 1-14, the Applicant amended claims 1-14 in a Response dated October 11, 2006. In response to a final Office Action dated December 20, 2006, the Applicant filed a Response (after final rejection) dated February 20, 2007, which made arguments and resubmitted amendments to the claims made in the previous Response dated October 11, 2006. An Advisory Action dated March 12, 2007 recited that the Response (after final rejection) was considered but did not place the application in condition for allowance. In response to the Advisory Action the Applicant filed a Request for Continued Examination dated April 12, 2007, which made arguments but did not amend the claims further. In response to a non-final Office Action dated July 18, 2007, the Applicant filed a Response dated October 16, 2007 which amended a claim to address a 35 USC 101 rejection. In response to a final Office Action dated January 8, 2008, the Applicant filed a Notice of Appeal on March 10, 2008. The claims as finally rejected are reproduced in an Appendix hereto (section 8).

(4) STATUS OF AMENDMENTS

No amendment to the claims was proposed subsequent to the Final Office Action dated January 8, 2008.

(5) SUMMARY OF CLAIMED SUBJECT MATTER

The present invention is in the context of authenticating a user of an electronic device in a variety of contexts and in a centralized manner. A context comprises all those events in mobile commerce services and applications the user is able to use in the electronic device. An embodiment of the present invention is to identify the context the user has selected for use and to select the user profile corresponding to said context. The user profiles comprise user keys for authentication and digital signing, and user certificates for access to said contexts or to authenticate itself in said contexts, and are stored in a centralized register in the electronic device. They are linked to each other so that there is a link between a particular context and a corresponding user profile. When the user selects the particular context, a device according to the present invention is able to automatically identify said context of use and select a corresponding user profile for accessing the user to said context or authenticating the user in said context by using said user profile.

Examples of the written description are summarized below.

When the user is at work he/she uses a work context in his/her device. A Work context is e.g. for an employee's corporate access security. When the user leaves from work and goes to his/her car he changes the context in use to a Drive context, which is for car access and car security setting/disabling. The user next goes to e.g. the grocery shop to buy some food and changes again the context in use to a Shop context which is for user authentication of personal retail transactions. Similarly when the user comes home and changes the context in his device to the Home context that is the context for residence access and alarm controlling. Further, in accordance with an exemplary embodiment of the present invention the user does not have to worry about how the device will appropriately authenticate them e.g. for corporate, home, car or shop. The application will select the appropriate level of security, the appropriate certificate information, and so on. Similarly there can be the concept of an application for teenagers devices that require additional security services, e.g. there can be contexts like School, Home, PopShop, Pals, Private chat groups, and so on.

(5A) INDEPENDENT CLAIMS (except means plus function claim 7)

Claims 1, 7, 13, and 14 are independent, of which claim 1 is drawn to a method, claims 7 and 13 are drawn to an electronic device, and claim 14 is drawn to a computer readable medium encoded with a computer program executable by a processor. Only independent claim 7 and claims 8-12 that depend from claim 7 recite in means plus function format.

The independent claims recite substantially similar subject matter. The elements of a method *for authenticating a user of an electronic device in a plurality of usage contexts the user is able to use with the electronic device* as in claim 1 below are bulleted and italicized, followed by details and text support for the claim element.

- *maintaining a centralized register of the usage contexts available for the electronic device and pre-stored user profiles, each user profile being associated with at least one usage context;*

This may be maintained as "a security element in the device wherein a register comprising user keys and user certificates are located," as in "the memory of the device [where] there is securely stored a centralized register of identifiers of the usage contexts such as services and/or applications available to the user of the device. The identifiers of the contexts register are linked to those user keys and user certificates in the security element register," (page 4, lines 9-14).

- *the electronic device entering a particular one of said plurality of usage contexts, said particular one being a selected usage context*;

"The usage context as disclosed is an application, like a banking application or web browser for example. [Thus] the user starts the application i.e. selects the usage context," (page 3, line 33 to page 4, line 2). This directly supports dependent claim 4, where the selected usage context comprises an event in a service or application, said event comprising at least one of an authentication event and verifying event, (page 5 lines 27-31).

- *the electronic device identifying said entering;*

"Figure 2 illustrates an electronic device according to an embodiment of the present invention. The device 200 comprises a processor 201 and a memory 202 that can be e.g. read-only-memory (ROM) or random access memory (RAM) for processing the tasks of the device. The device 200 may further comprise one or several applications 203, for performing various tasks in the device 200 [...] The application further comprises a computer program code for identifying a usage context selected by the user, a computer program code for selecting at least one user profile in response to the identified service, and a computer program code for authenticating the user in the selected service in response to the selected user profile," (page 6, lines 4-25).

- *selecting from the centralized register a user profile in response to said identifying; and*

"If the authenticating application identifies (step 102) the usage context the user has selected, it automatically selects the appropriate user profile, e.g. user key and user certificate to be used in said usage context. The user is notified of the selected user profile," (page 4, lines 15-19).

- *performing authentication in the selected usage context by using data from the selected user profile.*

"The user profile is linked to said usage context in use e.g. in the memory or in the appropriate security element (which requires authentication access) of the device (step 103) and provides the user profile such as user key and the user certificate to the usage context (step 104)," (page 4, lines 19-22). "If the application is not able to identify the usage context in step 102, it checks in step 105 whether said usage context is used for the first time," (page 4, lines 15-24 and Fig. 1). "If the usage context is being used for the first time (step 105), the application prompts the user for the user profile (the user key and the user certificate) to be used with the usage context (step 106) by acquiring the key and the certificate e.g. from service or a certificate authority," (page 4, lines 22-28 and Fig. 1). "If the usage context is not identified as a first time usage context in step 105, the application provides a selection of user profiles from the security element to the user (step 109)," (page 5, lines 20-24 and Fig. 1).

Independent claim 13 recites an electronic device for the above claim elements (e.g.: register at 202 of Fig. 2; interface at 204 of Fig. 2; processor 201 of Fig. 2), shown in Figure 2 and described on page 6, lines 4-11. The "means for ..." the above elements are recited in the electronic device claim 7.

Independent claim 14 recites a computer readable medium encoded with a computer program executable by a processor embodied on the electronic device to perform actions of the above claim elements is described on page 6, lines 21-25. Such a medium is shown at Fig. 2 as memory 202 with a program executable by the processor 201.

(5B) DEPENDENT CLAIMS (except means plus function claims 8-12)

Claim 2 recites wherein the selected user profile comprises at least one of the following: a user key, a user certificate. The written description discloses at page 4 lines 19-22 that the device 103 provides the user profile such as user key and the user certificate to the usage context (step 104).

Claims 3 recites wherein said user key further comprises at least one of the following a public key and a secret key. The written description discloses at page 5, line 31 to page 6 line 2 that certificates are automatically associated with key pairs (private key / public key) and because the keys themselves are cryptic, the user needs not to view or select the keys. Only the associated user-readable certificate information is viewable by the user.

Claim 4 recites wherein the selected usage context comprises an event in a service or application being used in the electronic device by the user, said event further comprising at least one of the following: authentication event, verifying event. The written description discloses at page 5 lines 4-5 a certificate request will be done from a mobile terminal for example like disclosed in the following manner. The service asks the user to authenticate. Further, the written description discloses on page 5, lines 27-31 that said key and certificate are available for the user to use in said usage context, e.g. for authenticating the user to access to the usage context such as a service or authenticating an event, like a transaction event in the usage context, like a shopping service.

Claims 5 recites authenticating a user's identity when accessing to the selected usage context. The written description discloses on page 6, lines 21-25 a computer program code for identifying a usage context selected by the user, a computer program code for selecting at least one user profile in response to the identified service, and a computer program code for authenticating the user in the selected service in response to the selected user profile.

(5C) MEANS PLUS FUNCTION CLAIMS

Claims 7-12 recite means plus function language. The following clauses from independent claim 7 are re-printed with added parenthetical citations to portions of the written description and drawings that support the related clause:

- *a centralized register of the usage contexts available for the electronic device and pre-stored user profiles, each user profile being associated with at least one usage context*, (application 208 at page 6, lines 17-19 and Figure 2; a computer program disclosed at page 6, lines 21-25, and signature button 403 and authentication button 404 page 8, lines 1-4 and Figure 4),
- *entering means for entering a particular one of said plurality of usage contexts, said particular one being a selected usage context*, (keyboard 204 and display 205 disclosed at page 6, lines 8-10; software application 208 page 6, lines 10-11, Figure 2, phone 200 page 8, lines 15-21 and Figure 3, display 401 and keyboard 402 page 7 line 33 to page 8 line 1, and Figure 4),
- *identifying means for identifying said entering*, (WAP identity module or a secure ASIC page 6, lines 12-17, Figure 4, and phone 200 page 8, lines 15-21 and Figure 3),
- *selecting means for selecting from the centralized register a user profile in response to said identifying*, (keyboard 204 page 6, lines 8-10 and Figure 2, and display 401 and keyboard 402 page 7 line 33 to page 8 line 1, and Figure 4), and
- *performing means for performing authentication in the selected usage context by using data from the selected user profile*, (computer program on electronic device 200 page 6, lines 21-25, digital signature button 403 and user authentication button page 8, lines 7-9 and Figure 4).

Support for means plus function elements of dependent claims 8-12 are set forth below in parentheses.

- Claim 8: *performing means are arranged to perform said authentication by using said data from the selected user profile to authenticate the user's identity when accessing the user to the selected usage context,* (Application 208 at page 6 lines 29-32 and Figure 2, phone 200 User Profile Manager at page 8 lines 15-21 and Figure 4);
- Claim 9: *performing means are arranged to perform said authentication by using said data from the selected user profile to authenticate a transaction made by the user in the selected usage context,* (application 208 page 6 lines 17-21 and Figure 2, and phone 200 and button 404 at page 8 lines 28-34 and Figure 4);
- Claim 10: *wherein said user profile comprises at least one of the following: user key and user certificate*, (application 208 page 6 lines 30-31, and phone 200 page 8 lines 31-34);
- Claim 11: *wherein said user key further comprises public key and secret key*, (page 5, line 31 to page 6 line 2);
- Claim 12: *wherein said electronic device is a mobile communication device*, (mobile communications device 400 page 7 lines 33-34 and Figure 4).

(6) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Issue A. Claims 1, 4-9 and 13-14 stand rejected under 35 U.S.C. § 103(a) as obvious over the combination of See (US 6,874,090) and Banatre (US 20020028683).

Issue B. Claims 2-3 and 10-12 stand rejected under 35 U.S.C. § 103(a) as obvious over the combination of See and Banatre further in view of Hanna (US 6,263,434).

(7) ARGUMENT

In the arguments below, claims argued separately are deemed not to fall with other claims in the group.

<u>Issue A. Obviousness of Claims 1, 4-9 and 13-14 over See and Banatre:</u>

Claim 1: Independent method claim 1 recites in relevant part:

selecting from the centralized register a user profile in response to said identifying, (The Appellant notes that "said identifying" is related to identifying **entering a particular one of a plurality of usage contexts** as previously recited similarly in the independent claims of the present application) *and*

performing authentication in the selected usage context by using data from the selected user profile.

The Appellant asserts that neither See nor Banatre alone or in combination disclose at least these claim elements.

Independent claims 7, 13, and 14 stand or fall with claim 1. All dependent claims under Issue A are argued separately.

In the final Office Action the Examiner indicates that See discloses in column 8 lines 15-48 the following feature recited similarly in the independent claims of the present application:

> *"<u>selecting from the centralized register</u> a user profile <u>in response to said identifying</u>, and performing authentication in <u>the selected usage context</u> by using data from the selected user profile"*

As stated above, the Appellant notes that "said identifying" is related to identifying **entering a particular one of a plurality of usage contexts** as previously recited similarly in the independent claims of the present application.

See relates to a method of regulating connectivity to and within a communication network. In See an authentication server stores user-specific entries. Each user-specific entry can include user identification information and a list of authorized network resources. In See the user information can contain a password of a user and the list of authorized network resources can be a list of identifiers of VLANs to which data-traffic originated by the user is authorized to access. Further in See, packets from the user targeted to an unauthorized network resource can be dropped or directed to a pre-determined network element for further actions.

In the final Office Action the Examiner states:

> "[See] does not expressly disclose the electronic device entering a particular one of said plurality of usage contexts, the electronic device identifying said entering," (emphasis added); and
>
> "Banatre et al. however does disclose the electronic device entering a particular one of said plurality of usage contexts, the electronic device identifying said entering (see US PGPub'683: p. 2, [0029], [0031]: request/answer for content sensitive service)" (emphasis added).

The Appellant notes that in the Response filed October 16, 2007 argument was presented stating that at least for the reason that the Examiner's expressly admits See does not disclose "entering" and "identifying said entering," as stated above, then as a logical consequence See clearly can not be seen to disclose or suggest at least "**selecting from the centralized register a user profile in response to said identifying**," as previously asserted in the rejection by the Examiner.

Regarding this argument in the Response to Arguments section of the final Office Action dated January 8, 2008 the Examiner states:

> "It is Applicant's argument that at least for the reason the Examiner's admits See does not disclose "entering" and "identifying said entering," then as a logical consequence See clearly can not be seen to disclose or

> suggest at least "selecting from the centralized register a user profile in response to said identifying, and performing authentication in the selected usage context by using data from the selected user profile" as in claim 1.The Examiner respecifully disagrees. See discloses a method for authenticating a user to personalized user resources. Each resource has an associated user defined by a user identifier (see column 7, lines 52-55). See further discloses that when a resource is selected for access, and a match between the resource and user (i.e. process of authentication) is found, a communication link is generated to facilitate access (see column 8, lines 15-48)," (emphasis added).

As cited See actually discloses:

> "Means 510 stores each user-specific entry as a related pair in user records 330. Each user-specific entry preferably includes user identifier information and a list of authorized network resources. User-specific entries may also include time restrictions for the particular user. User identification information preferably includes signature information for the user, such as a password," (emphasis added), (col. 7, lines 52-58); and

> "Server 320 also includes ID VER means 530. Means 530 serves to subject to a verification process authentication information received from users via agent 400. Means 530, upon receipt of authentication information from agent 400, determines if the log-in response matches the user identification information associated with a user-specific entry in user records 330. If a match is found, and there are time restrictions associated with the user-specific entry, means 530 determines from the time restrictions if the user is authorized to use network 1 at the particular time," (emphasis added), (col. 8, lines 15-23).

Firstly, the Appellant submits that the user-specific entries disclosed in See which include identification information and time restrictions clearly can not be used to disclose or suggest "a centralized register of the usage contexts available for the electronic device and pre-stored user profiles, each user profile being associated with at least one usage context," as appears to be indicated by the Examiner in the rejection of claim 1. The Appellant contends that nowhere is See is there found to be disclosed or suggested that the user identifier information is associated with a particular usage context being selected as in claim 1.

Further, as cited by the Examiner See appears to disclose a log-in response is accepted **before** the user identification information associated with the user-specific entries is checked for a match. The Appellant submits it appears that in order to support the rejection the Examiner is improperly rearranging the order of elements in claim 1 to fit the suggestions asserted by the Examiner. The Appellant submits that contrary to See claim 1 relates to maintaining a centralized register of the usage contexts and pre-stored user profiles, each user profile being associated with at least one usage context, entering a particular one of said plurality of usage contexts which is identified as a selected usage context, **selecting from the centralized register a user profile in response to said identifying**, and **then** **performing authentication** in the selected usage context by using data from the selected user profile. The Appellant contends that the user-specific entry that contains a user profile (user identifier) in See is selected on the basis of matching with the log-in response, and is not selected in response to identifying entering a particular one of a plurality of usage contexts as is claimed.

In addition, in the final Office Action the Examiner states Banatre "does disclose the electronic device entering a particular one of said plurality of usage contexts, the electronic device identifying said entering (see US PGPub '683: p. 2, [0029],[0031]: request/answer for content sensitive service)."

Firstly, the Appellant contends that Banatre can not be seen to address a short fall of See as stated above.

The relevant and cited teachings of Banatre relate to an ad hoc mobile network installed on a train. In Banatre when a user gets on the train and within a perimeter of the ad hoc network he can access that ad hoc network and book his train service, (par. [0082]). The Appellant contends that if this is meant to disclose or suggest a "context" as applied in the rejection of claim 1 then it clearly fails for at least the reason that this context is not stored with a user profile which is associated to the context. In Banatre the users portable device merely senses it is within reach of the ad hoc network. In addition, at least for the reason that the network is ad hoc there is seen to be no centralized register for storage of a context and associate user profile as in claim 1. Further, in Banatre there appears to be no need for authentication or a need to store information with identification information as in See. The Appellant contends that the ad hoc network in Banatre which is described to be used on a train is not seen to have reason to restrict access as in claim 1. As it appears to be disclosed in Banatre any rider can have access to the ad hoc network and there is no means to exclude any person attempting access to that ad hoc network.

Further, for at least these reasons a person skilled in the art would not be motivated to combine the references cited as the combination would still not disclose or suggest the independent claims of the present application. In addition, the Appellant contends that such a combination, though not agreed as proper, would at least improperly change the principles operation of See (the principle by which a user specific entry is selected). Moreover, such a combination would require an inventive step not present in either reference in order to disclose or suggest the independent claims of the present application.

The Appellant submits that in the solution recited in the independent claims of the present application the fact that the user profile is selected in response to identifying entering to a particular usage context is significant, at least because it opens a door for a solution in which a device is able to automatically select or suggest an appropriate user profile for giving to a user an access to a context or authenticating the user in said context. Thus, in an exemplary embodiment of the invention the user does not have to manually select a user key, a user certificate, or the like.

On the basis of the above-presented review, the Appellant contends that neither See nor Banatre, separately or combined, solve a technical problem that is solved by the solution recited in the independent claims of the present application.

Claim 4 depends from claim 1, and recites "*wherein the selected usage context comprises an event in a service or application being used in the electronic device by the user, said event further comprising at least one of the following: authentication event, verifying event.*" As cited See discloses that the agent relays log-in responses received from the system to a basic authentication server in the network for verification of the user. (col. 3 lines 7-9), but fails to disclose any further particulars as to an event in a service or application *in the selected usage context* being used in an electronic device by the user.

Claim 5 depends from claim 1 and recites wherein the authentication comprises authenticating user's identity when accessing to the selected usage context. As cited See discloses "Server 320 also includes ID VER means 530. [and] Means 530 serves to subject to a verification process authentication information received from users via agent 400," (col. 8, lines 15-18). The Appellant submits that here See does not disclose or suggest at least where claim 5 recites "when accessing to the selected usage context."

Claim 6 depends from claim 1 and recites wherein the authentication comprises authenticating a transaction made by the user in the selected usage context. As cited See discloses "the user enters a log-in response and the response is transmitted to agent 400 (915)," (col. 11 lines 18-19), but fails to disclose any further particulars as a selected usage context. No disclosure in Jin is seen respecting a selected usage context.

Dependent Claim 8 recites wherein said performing means are arranged to perform said authentication by using said data from the selected user profile to authenticate the user's identity when *accessing the user to the selected usage context.* The Appellant notes that the Examiner does not appear to cite support in a reference for the rejection of claim 8. The Appellant contends that for at least the reasons already stated the references cited are not seen to disclose or suggest at least where claim 8 recites in part *accessing the user to the selected usage context.*

Dependent claim 9 recites wherein said performing means are arranged to perform said authentication by using said data from the selected user profile to authenticate a transaction made by the user in the selected usage context. The Appellant notes that the Examiner does not appear to cite support in a reference for the rejection of claim 9. The Appellant contends that for at least the reasons already stated the references cited are not seen to disclose or suggest at least where claim 9 recites in part *to authenticate a transaction made by the user in the selected usage context.*

Issue B. OBVIOUSNESS OF CLAIMS 2-3 AND 10-12 OVER SEE AND BANATRE IN VIEW OF HANNA:

Dependent claims 10 and 11 stand or fall with dependent claims 2 and 3, respectively.

Dependent claim 2 recites:

A method according to claim 1, wherein the selected user profile comprises at least one of the following: a user key, a user certificate.

The Appellant notes that in claim 1, from which claim 2 depends, the user profile is selected in response to identifying an entering of one of a plurality of usage contexts. The Appellant contends that for at least the reasons already stated none of the references cited can be seen to disclose or suggest ate least where claim 2 recites in part "*the selected user profile*."

Dependent claim 3 recites:

A method according to claim 2, wherein said user key further comprises at least one of the following a public key and a secret key.

The Appellant contends that for at least the reasons already stated and the reason that claim 3 depends from claim 2, the references cited can not be seen to disclose or suggest claim 3.

Pursuant to 35 USC 41.37, a CLAIMS APPENDIX, EVIDENCE APPENDIX, and RELATED PROCEEDINGS APPENDIX follow the certificate of mailing below.

For at least the above reasons, the Appellants contend that See, Banatre and the Hanna reference, alone or in combination with one another or ordinary skill in the art, anticipate or render obvious any of the fourteen claims argued above. The Appellants respectfully requests the Board reverse the final rejection in the Office Action of December 14, 2005, and further that the Board rule that the pending claims are patentable over the cited art.

Respectfully submitted:

June 6, 2008

John A. Garrity
Date

Reg. No.: 60,470
Customer No.: 29683
HARRINGTON & SMITH, PC
4 Research Drive
Shelton, CT 06484-6212
Telephone: (203)925-9400
Facsimile: (203)944-0245
email: jgarrity@hspatent.com

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450.

June 6, 2008

Date
Name of Person Making Deposit

(8) CLAIMS APPENDIX

Listing of Claims:

1. (Previously Presented) A method for authenticating a user of an electronic device in a plurality of usage contexts the user is able to use with the electronic device, the method comprising:

maintaining a centralized register of the usage contexts available for the electronic device and pre-stored user profiles, each user profile being associated with at least one usage context,

the electronic device entering a particular one of said plurality of usage contexts, said particular one being a selected usage context,

the electronic device identifying said entering,

selecting from the centralized register a user profile in response to said identifying, and

performing authentication in the selected usage context by using data from the selected user profile.

2. (Previously Presented) A method according to claim 1, wherein the selected user profile comprises at least one of the following: a user key, a user certificate.

3. (Previously Presented) A method according to claim 2, wherein said user key further comprises at least one of the following a public key and a secret key.

4. (Previously Presented) A method according to claim 1, wherein the selected usage context comprises an event in a service or application being used in the electronic device by the user, said event further comprising at least one of the following: authentication event, verifying event.

5. (Previously Presented) A method according to claim 1, wherein the authentication comprises authenticating user's identity when accessing to the selected usage context.

6. (Previously Presented) A method according to claim 1, wherein the authentication comprises authenticating a transaction made by the user in the selected usage context.

7. (Previously Presented) An electronic device for authenticating a user of said electronic device in a plurality of usage contexts the user is able to use with the electronic device, the electronic device comprising:

a centralized register of the usage contexts available for the electronic device and pre-stored user profiles, each user profile being associated with at least one usage context,

entering means for entering a particular one of said plurality of usage contexts, said particular one being a selected usage context,

identifying means for identifying said entering,

selecting means for selecting from the centralized register a user profile in response to said identifying, and

performing means for performing authentication in the selected usage context by using data from the selected user profile.

8. (Previously Presented) An electronic device according to claim 7, wherein said performing means are arranged to perform said authentication by using said data from the selected user profile to authenticate the user's identity when accessing the user to the selected usage context.

9. (Previously Presented) An electronic device according to claim 7, wherein said performing means are arranged to perform said authentication by using said data from the selected user profile to authenticate a transaction made by the user in the selected usage context.

10. (Previously Presented) An electronic device according to claim 8, wherein said user profile comprises at least one of the following: user key and user certificate.

11. (Previously Presented) An electronic device according to claim 10, wherein said user key further comprises public key and secret key.

12. (Previously Presented) An electronic device according to claim 11, wherein said electronic device is a mobile communication device.

13. (Previously Presented) An electronic device for authenticating a user of said electronic device in a plurality of usage contexts the user is able to use with the electronic device, the electronic device comprising:

a centralized register of the usage contexts available for the electronic device and pre-stored user profiles, each user profile being associated with at least one usage context,

an interface for entering a particular one of said plurality of usage contexts, said particular one being a selected usage context,

a processor configured to:

identifying said entering,

selecting from the centralized register a user profile in response to said identifying, and

performing authentication in the selected usage context by using data from the selected user profile.

14. (Previously Presented) A computer readable medium encoded with a computer program executable by a processor to perform actions ~~for~~ of an electronic device for authenticating a user of said electronic device in a plurality of usage contexts the user is able to use, the actions comprising:

maintaining a centralized register of the usage contexts available for the electronic device and pre-stored user profiles, each user profile being associated with at least one usage context,

entering to a particular one of said plurality of usage contexts, said particular one being a selected usage context,

identifying said entering,

selecting from the centralized register a user profile in response to said identifying, and

performing authentication in the selected usage context by using data from the selected user profile.

END OF CLAIMS

(9) EVIDENCE APPENDIX

Subsequent to this page are attached the following references:

U.S. Patent No. 6,874,090 to See, et al.

U.S. Publication No. 2002/0028683 of Banatre et al.

US Patent No. 6,263,434 to Hanna et al.

(10) RELATED PROCEEDINGS APPENDIX

None.